UNITED STATES DISTRICT COURT
DISTRICT OF NEW HAMPSHIRE

IN THE MATTER OF THE SEARCH OF SEVENTEEN (17) ELECTRONIC DEVICES SEIZED FROM 4 PINK STREET, ROCHESTER, NEW HAMPSHIRE 03867 CURRENTLY LOCATED AT THE BEDFORD RESIDENT AGENCY, BEDFORD, NH	Case No. 23-mj-102-01/17-AJ

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Kimberly Blackwood, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—**the electronic devices and data** described in Attachment A (hereinafter, "DEVICES")—which are currently in the possession of law enforcement within the District of New Hampshire, and for the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent employed by the Federal Bureau of Investigation ("FBI"). I have been so employed since October 2000 and am currently assigned to the Boston Field Office, Bedford Resident Agency of the FBI. I am an investigative or law enforcement officer of the United States within the meaning of 18 U.S.C. § 2510(7), in that I am empowered by law to conduct investigations and to make arrests for federal felony offenses.

3. Since becoming a Special Agent with the FBI, my duties and responsibilities have included, but are not limited to, conducting various violations of federal laws, specifically criminal child exploitation investigations, and enforcement of federal laws. As a Special Agent with the FBI,

I have received basic criminal investigator training as well as specialized training in the investigation of child exploitation matters.

4. The facts in this affidavit come from my personal observations and review of records, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that evidence and instrumentalities of violations of Title 18 United States Code Section 2252A – Distribution, Receipt, and Possession of Child Pornography are located on the DEVICES described in Attachment A. There is also probable cause to search the DEVICES described in Attachment A for evidence and instrumentalities of these crimes further described in Attachment B.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is "a courtof competent jurisdiction" as defined by 18 U.S.C. § 2711. *See* 18 U.S.C. §§ 2703(a), (b)(1)(A), (c)(1)(A). Specifically, the Court is "a district court of the United States … that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

RELEVANT STATUTORY PROVISIONS

7. **Distribution or Receipt of Child Pornography**: 18 U.S.C. § 2252A(a)(2) provides that it is a crime to knowingly receive or distribute any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

8. **Possession of Child Pornography**: 18 U.S.C. § 2252A(a)(5) provides that it is a crime to knowingly possess, or knowingly access with intent to view, any child pornography that

has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

9. **Child pornography or Child abusive material** means any visual depiction, in any format, of sexually explicit conduct where: (A) the production involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital or computer-generated image that is substantially indistinguishable from that of a minor engaged in sexually explicit conduct; or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. *See* 18 U.S.C. § 2256(8).

10. **Visual depictions** include undeveloped film and videotape, and data stored on computer disk or by electronic means, which are capable of conversion into a visual image, and data which are capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format. *See* 18 U.S.C. § 2256(5).

11. **Minor** means any person under the age of eighteen years. *See* 18 U.S.C. § 2256(1).

12. **Sexually explicit conduct** means actual or simulated: (i) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (ii) bestiality; (iii) masturbation; (iv) sadistic or masochistic abuse; or (v) lascivious exhibition of the genitals or pubic area of any person. *See* 18 U.S.C. § 2256(2).

TECHNICAL TERMS

13. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. **Computer**, as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1) as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions and includes any data storage facility or communications facility directly related to or operating in conjunction with such

device."

b. **Storage Medium**: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

c. **Wireless Telephone**: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

d. **Smartphone:** A portable personal computer with a mobile operating system having features useful for mobile or handheld use. Smartphones, which are typically pocket-sized (as opposed to tablets, which are larger in measurement), have become commonplace in modern society in developed nations. While the functionality of smartphones may vary somewhat from model to model, they typically possess most if not all of the following features and capabilities: 1) place and receive voice and video calls; 2) create, send and receive text messages; 3) voice-activated digital assistants (such as Siri, Google Assistant, Alexa, Cortana, or Bixby) designed to enhance the user experience; 4) event calendars; 5) contact lists; 6) media players; 7) video games; 8) GPS navigation; 9) digital camera and digital video camera; and 10) third-part software components commonly referred to as "apps." Smartphones can access the Internet through cellular as well as Wi-Fi ("wireless fidelity") networks. They typically have a color display with a graphical user interface that covers most of the front surface of the phone and which usually functions as a touchscreen and sometimes additionally as a touch-enabled keyboard.

e. **SIM Card**: Stands for a "subscriber identity module" or "subscriber identification module," which is the name for an integrated circuit used in mobile phones that is designed to securely store the phone's international mobile subscriber identity (IMSI) number and its related key, which are used to identify and authenticate subscribers on mobile telephony devices (such as mobile phones and computers). It is also possible to store contact information on many SIM cards.

f. **Log Files**: Records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain.

For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

g. **Internet**: A global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

h. **Internet Protocol Address (IP address)**: A unique number used by a computer to access the Internet. Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static–that is, long-term–IP addresses, while other computers have dynamic that is, frequently changed–IP addresses. Internet providers use either IP version 4 or more recently IP version 6. IPv4 is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Given the rapid growth of the volume of internet-enabled devices over the past two decades, in early 2011, the Internet Assigned Numbers Authority exhausted the global IPv4 free pool. As such, many providers switched to IPv6, which is a series of eight hexadecimal digits, each separated by colons (e.g., FFE:FFFF:7654:FEDA:1245:BA98:3210:4562).

i. The terms "**records**," "**documents**," and "**materials**," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks ("DVDs"), Personal Digital Assistants ("PDAs"), Multi Media Cards ("MMCs"), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage devices).

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

14. As described above and in Attachment B, this application seeks permission to search for records that might be found on the DEVICES, in whatever form they are found. The warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

15. *Probable cause.* I submit that there is probable cause to believe records will be stored on the DEVICES, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. Depending on a variety of factors, a particular computer could easily not overwrite deleted files with new data for many months, and in certain cases conceivably ever.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence,

because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

16. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on the DEVICES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-

mail address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

17. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy

of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

18. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the DEVICES consistent with the warrant. The examination may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

19. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize the execution of the warrant at any time in the day or night.

CHARACTERISTICS OF COLLECTORS OF CHILD PORNOGRAPHY

20. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the collection of child pornography (hereinafter, "collectors").

21. Collectors may receive sexual stimulation and satisfaction from contact with children, or from having fantasies of children engaged in sexual activity or suggestive poses, or from literature describing such activity.

22. Collectors may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides, drawings, and/or other visual media. Collectors typically use these materials for their own sexual arousal and gratification. Collectors often have companion collections of child erotica. Child erotica are

materials or items that are sexually suggestive and arousing to pedophiles, but which are not in and of themselves obscene or pornographic. Such items may include photographs of clothed children, drawings, sketches, fantasy writings, diaries, pedophilic literature, and sexual aids.

23. Collectors who also actively seek to engage in sexual activity with children may use these materials to lower the inhibitions of a child they are attempting to seduce, convince the child of the normalcy of such conduct, sexually arouse their selected child partner, or demonstrate how to perform the desired sexual acts.

24. Collectors almost always possess and maintain their "hard copies" of child pornographic images and reference materials (*e.g.*, mailing and address lists) in a private and secure location. With the growth of the internet and computers, many collections are maintained in digital format. Typically, these materials are kept at the collector's residence for easy access and viewing. Collectors usually place high value on their materials because of the difficulty, and the legal and social danger, associated with acquiring them. As a result, it is not uncommon for collectors to retain child pornography for long periods, even for years. Collectors often discard child pornography images only while "culling" their collections to improve their overall quality.

25. Collectors also may correspond with and/or meet others to share information and materials. They may save correspondence from other child pornography distributors/collectors, including contact information like email addresses, and may conceal such correspondence as they do their sexually explicit material.

26. Collectors prefer not to be without their child pornography for any prolonged periods of time. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

27. Subscribers to websites that are primarily designed to provide child pornography have a strong likelihood of being collectors of child pornography. This high degree of correlation

between subscription and collection behavior has been repeatedly confirmed during nationwide law enforcement initiatives.

28. In sum, collectors of child pornography frequently maintain their collections in a private and secure location such as their residence, often in digital format, for long periods of time. They also maintain information related to their receipt or distribution of such media in that location, including correspondence with and contact information for other individuals distributing or sharing child pornography.

PROBABLE CAUSE

29. The Federal Bureau of Investigation (FBI), Internal Revenue Service (IRS), and U.S. Treasury Inspector General for Tax Administration (TIGTA) are investigating, HEATH GAUTHIER in connection with a CARES Act loan fraud scheme. In response to the coronavirus (COVID-19) pandemic and economic crisis, Congress passed the Coronavirus Aid, Relief, and Economic Security (CARES) Act. The CARES Act allowed businesses to obtain loans to provide economic assistance during the COVID-19 pandemic.

30. On February 15, 2023, a federal grand jury returned an indictment charging GAUTHIER with six counts of wire fraud and attempted wire fraud, in violation of 18 U.S.C. §§ 1349, 1343, and three counts of aggravated identity theft, in violation of 18 U.S.C. § 1028A (collectively hereafter "the Fraud Offenses"). *United States v. Gauthier*, 23-cr-15-JL. The indictment alleges that GAUTHIER used the identities of other individuals, and created false tax and other documents, to fraudulently apply for CARES Act loans.

31. Based on the facts gathered regarding the Fraud Offenses, federal agents obtained a search warrant for GAUTHIER's residence and his person. *See In re Search of 4 Pink Street, Rochester, New Hampshire and the Person of Heath Gauthier*, Case No. 23-mj-27-01-AJ (District of New Hampshire, issued February 14, 2023). That warrant authorized the search of

GAUTHIER's residence and person, and the seizure and search of, among other items, electronic devices used as means to commit the Fraud Offenses. The warrant also authorized the off-site forensic examination of those devices.

32. Law enforcement executed the premises search warrant at GAUTHIER's residence on February 16, 2023. During the execution of the warrant, agents found and seized various electronic devices, including the DEVICES listed in Attachment A. Among those DEVICES was GAUTHIER's cellular telephone, described as an Android, Motorola, Moto Z3 Play. Law enforcement conducted an initial review on the device known as triaging. During the review, agents discovered that the browser application was open to a website with the name "www.thegay.com". On the web page was a video captioned, "Teen Boy Violated His Sister's Drunk Boyfriend During His Birthday Party." Agents did not view the video at that time.

33. Following the execution of the search warrant, the DEVICES have remained in the possession of law enforcement while awaiting further analysis. Subsequently, a computer forensic examiner extracted digital data from the seized devices for later review by the case agents.

34. On May 17, 2023, during the review of electronic devices seized during the search of GAUTHIER's residence, in particular a hard drive described as EXHIBIT 004: Western Digital My Book 1110 external drive; SN: WCAV5J746167; size: 1 GB, TIGTA Special Agent Michael Nunley observed in plain view a series of images depicting apparent child pornography. Special Agent Nunley ceased his review pending my review to determine if there was probable cause to seek an additional warrant to search for evidence related to criminal child pornography offenses.

35. On May 24, 2023, I reviewed the series of images observed by SA Nunley during his review of the contents of the hard drive referenced in paragraph 34, above. Specifically, I observed the following images in a folder named My Book\Heath's\WindowImageBackup\MSR-PC\Backup 2014-07-17 222603\e55ddac4-5ee2-11e3-8d59-806e6f6e6963.vhd:

a. An image with the Item ID 1595262, depicting an anus of a prepubescent male with a hand holding the prepubescent male's scrotum. A penis is penetrating the prepubescent male's anus and this another hand on the prepubescent male's buttocks. The bottom of this image reads, "BoyExtra." This image is attached as Exhibit 1 to this affidavit.[1]

b. An image with the Item ID 1595197, depicting a naked prepubescent male licking an adult penis. There is another penis penetrating this prepubescent male's anus. This image is attached as Exhibit 2 to this affidavit.

c. An image with the Item ID 1595035, depicting a prepubescent male with a penis in his mouth holding another adult penis in his hand. The bottom of this image reads, "Boyztube.com." This image is attached as Exhibit 3 to this affidavit.

d. An image with the Item ID 1594551, depicting a shirtless prepubescent male and a naked adult male. The adult male is ejaculating on the face of the prepubescent male and holding the prepubescent male's head/hair. The prepubescent male is turning his head away from the ejaculation stream. The bottom of this image reads, "boy3k.com." This image is attached as Exhibit 4 to this affidavit.

36. I concluded that the individuals in above images were prepubescent based on the following observations: The individuals did not have any pubic hair on their visible armpits, chests, or genital areas. The individuals also had young facial features, stature, and undeveloped muscles.

37. Because the child pornography was discovered in an external hard drive, another electronic device necessarily had to have been used to back up or transfer that material to the external hard drive.

[1] Exhibits 1 through 4 are stored in a secured location at the U.S. Attorney's Office.

38. In my training and experience, collectors of child pornography frequently have multiple devices used to store or transfer child pornography. Accordingly, there is probable cause to believe that another device or devices seized from GAUTHIER's residence, as listed in Attachment A, contains evidence of the receipt, distribution, and/or possession of child pornography.

ADDITIONAL INFORMATION REGARDING GAUTHIER

39. Based on information obtained from open source and law enforcement databases, GAUTHIER was arrested on October 16, 2004, when he traveled to Keene, New Hampshire in order to engage in sexual activity with a minor who was, in fact, an undercover law enforcement officer. As a result of the investigation, GAUTHIER pleaded guilty to violations of New Hampshire Code Sections 649-B:4 – Prohibited Use of Computer Services and 632-A:3 – Felonious Sexual Assault and was required to register as a sex offender.

40. On January 17, 2023, the National Center for Missing and Exploited Children received CyberTipline Report 153023682, which was submitted by PayPal, Inc, the parent company of Venmo. The report detailed suspicious activity regarding Venmo account 63162689, belonging to GAUTHIER, wherein multiple payments were made to the account of a minor male individual with transaction notes referring to "pics" and "meet up". The activity was flagged as potentially related to child sexual abuse material (CSAM), also known as child pornography.

CONCLUSION

41. Based on the forgoing, I submit that this affidavit supports probable cause for a warrant to search the location described in Attachment A for evidence and instrumentalities of violations of 18 U.S.C. §§ 2252A, 2256, further described in Attachment B.

Respectfully submitted,

Kimberly Blackwood
Special Agent, Federal Bureau of Investigation

Subscribed and sworn to before me on this 26th day of May 2023.

Honorable Andrea K. Johnstone
United States Magistrate Judge
District of New Hampshire

ATTACHMENT A

Property to Be Searched

This warrant applies to the electronic devices described as follows:

1. Seagate FreeAgent Go external drive; SN: 2GE6MXS5; size: 320.0 GB.
2. VICFUN flash drive; SN: NO-LABEL (USB Serial number: 1D2020005016103D); size: 16 GB
3. Western Digital My Passport 0748 external drive; SN: WXK1A9145428; size: 2 TB
4. Western Digital My Book 1110 external drive; SN: WCAV5J746167; size: 1 GB
5. Toshiba MK1059GSM external drive; SN: Z0GXTCT0T; size: 500 GB
6. Apple iPad (A2197) mobile device; SN: GG7CLCSYMF3M; IMEI: UNKNOWN; size: N/A; dark gray in color
7. Apple iPad (A1893) mobile device; SN: DMPXGJ4RJF8J; IMEI: UNKNOWN; size: N/A; gray in color
8. HGST HTS541075A9E680 drive; Serial Number (SN): 130507J813001XG4Z9YA; size: 750 GB from a Toshiba Satellite P75 computer: Serial Number (SN): 8D040167C; containing one drive
9. Motorola XT2041-4 Moto G Power mobile device; SN: N/A; IMEI: UNKNOWN; ICCID=8914800000 4337608262; size: N/A; black in color
10. Motorola Moto Z3 Play XT1929-4 mobile device; SN: ZY2252C8XL; IMEI: 3518 8609 0405 124; size: 64 GB; black in color
11. DELL flash drive; SN: NO-LABEL (USB Serial number: 040408030000001B33AE00000000000); size: 128 MB
12. THINKWARE DASH CAM MCM20N0611 MicroSD card; SN: NO-LABEL; size: 32 GB
13. Samsung EVO Select SD card; SN: KND77TNQH743; size: 64 GB
14. PNY MicroSD HC SD card; SN: UNKNOWN; size: 32 GB
15. Kingston SDCG2 SD card; SN: UNKNOWN; size: 64 GB
16. Motorola Edge plus (2022) XT2201-3 mobile device; SN: UNKNOWN; IMEI: 356439690571575; size: 8 GB; black in color

17. Apple iPad Pro (A2759) mobile device; SN: FW7QC22MYK; IMEI: UNKNOWN; size: 256 GB; gray in color

which are currently in the possession of the Federal Bureau of Investigation located in Bedford, New Hampshire. This warrant authorizes the forensic examination of the DEVICES for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

Particular Things to be Seized

1. All records relating to violations of 18 U.S.C. § 2252A, 2256, relating to the distribution, receipt, and possession of child pornography, including:

   a. Any and all visual depictions of minors;

   b. Any and all address books, names and lists of names and addresses of minors;

   c. Any and all diaries, notebooks, notes, and other records reflecting physical contacts, whether real or imagined, with minors; and

   d. Any and all child erotica, including photographs of children that are not sexually explicit, drawings, sketches, fantasy writings, diaries, and sexual aids.

2. Computers or storage media used as a means to commit the violations described above.

3. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

   a. Evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondences;

   b. Evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

   c. Evidence of the lack of such malicious software;

   d. Evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

   e. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER.

   f. Evidence of the times the COMPUTER was used;

   g. Passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

   h. Documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

   i. Records of or information about Internet Protocol addresses used by the

COMPUTER;

j. Records of, or information about, the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

k. Contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic

data to the custody and control of attorneys for the government and their support staff for their independent review.

If the government identifies seized communications to/from an attorney, the investigative team will discontinue review until a filter team of government attorneys and agents is established. The filter team will have no previous or future involvement in the investigation of this matter. The filter team will review all seized communications and segregate communications to/from attorneys, which may or may not be subject to attorney-client privilege. At no time will the filter team advise the investigative team of the substance of any of the communications to/from attorneys. The filter team then will provide all communications that do not involve an attorney to the investigative team and the investigative team may resume its review. If the filter team decides that any of the communications to/from attorneys are not actually privileged (e.g., the communication includes a third party or the crime-fraud exception applies), the filter team must obtain a court order before providing these attorney communications to the investigative team.

UNITED STATES DISTRICT COURT
DISTRICT OF NEW HAMPSHIRE

IN THE MATTER OF THE SEARCH OF SEVENTEEN (17) ELECTRONIC DEVICES SEIZED FROM 4 PINK STREET, ROCHESTER, NEW HAMPSHIRE 03867 CURRENTLY LOCATED AT THE BEDFORD RESIDENT AGENCY, BEDFORD, NH	Case No.

Placeholder for Exhibits 1, 2, 3, and 4.

The original exhibits are stored in a secured location at the U.S. Attorney's Office